CLAIMS

1. A method for providing a secret cryptographic key (sk) and a public cryptographic key (pk) applicable in a network of connected computer nodes using a signature scheme, the method being executable by a first computer node and comprising the steps of:

- generating the secret cryptographic key (sk) by
  - selecting two random factor values (P, Q),
  - multiplying the two selected random factor values (P, Q) to obtain a modulus value (N), and
  - selecting a secret base value (g', h', x') in dependence on the modulus value (N), wherein the secret base value (g', h', x') forms part of the secret cryptographic key (g', h', x');
- generating the public cryptographic key (pk) by
  - selecting a number (I) of exponent values (e_1,...,e_I), and
  - deriving a public base value (g, h, x) from the exponent values (e_1,...,e_I) and the secret base value (g', h', x'), wherein the public base value (g, h, x) and the modulus value (N) form part of the public cryptographic key (g, h, x, N);
- deleting the two random factor values (P, Q); and
- providing the public cryptographic key (g, h, x, N) within the network;

such that the public cryptographic key (g, h, x, N) and at least one of the selected exponent values (e_1,...,e_I) is usable for verifying a signature value (i, y, a) on a message (m) to be sent within the network to a second computer node for verification.

2. The method according to claim 1 further comprising providing a description of the exponent values (e_1,...,e_I) within the network.

3. The method according to any preceding claim further comprising defining an order of the selected exponent values (e_1,...,e_I) for enabling to communicate the validity of the signature value (i, y, a) in the event of a detected intrusion.

4. A method for providing a signature value (i, y, a) on a message (m) in a network of connected computer nodes, the method being executable by a first computer node and comprising the steps of:

- selecting a first signature element (a);
- selecting a signature exponent value (e_i) from a number (I) of exponent values $(e_1,...,e_I)$; and
- deriving a second signature element (y) from a provided secret cryptographic key (g'_i, h'_i, x'_i), the message (m), and the number (I) of exponent values $(e_1,...,e_I)$ such that the first signature element (a), the second signature element (y), and the signature exponent value (e_i) satisfy a known relationship with the message (m) and a provided public cryptographic key (g, h, x, N), wherein the signature value (i, y, a) comprises the first signature element (a), the second signature element (y), and a signature reference (i) to the signature exponent value (e_i),

the signature value (i, y, a) being sendable within the network to a second computer node for verification.

5. The method according to claim 4, wherein the step of deriving a second signature element (y) further comprises deriving a signature base value (g_i, h_i, x_i) using a provided public cryptographic key (g, h, x, N), the provided secret cryptographic key (g'_i, h'_i, x'_i), and the exponent values $(e_1,...,e_I)$.

6. The method according to claim 4 or 5 further comprising deriving a new secret cryptographic key $(g'_{i+1}, h'_{i+1}, x'_{i+1})$ from the provided secret cryptographic key (g'_i, h'_i, x'_i) and the selected signature exponent value (e_i).

7. A method for verifying a signature value (i, y, a) on a message (m) in a network of connected computer nodes, the method being executable by a second computer node and comprising the steps of:

- receiving the signature value (i, y, a) from a first computer node;
- deriving a signature exponent value (e_i) from the signature value (i, y, a); and

- verifying whether the signature exponent value (e_i) and part of the signature value (i, y, a) satisfy a known relationship with the message (m) and a provided public cryptographic key (g, h, x, N), otherwise refusing the signature value (i, y, a),

wherein the signature value (i, y, a) was generated from a first signature element (a), a number (l) of exponent values (e_1,...,e_l), a provided secret cryptographic key (g'_i, h'_i, x'_i), and the message (m).

8. A method for communicating within a network of connected computer nodes the validity of a signature value (i, y, a) in the event of an exposure of a secret cryptographic key (sk) relating to the signature value (i, y, a), the method comprising the steps of:

- defining an order of exponent values (e_1,...,e_l);

- publishing a description of the exponent values (e_1,...,e_l) and the order of the exponent values (e_1,...,e_l) within the network;

- publishing a revocation reference (j) to one of the exponent values (e_1,...,e_l) within the network such that the validity of the signature value (i, y, a) is determinable by using the revocation reference (j), the order of exponent values (e_1,...,e_l), and a provided public cryptographic key (pk).

9. The method according to any preceding claim further comprising applying each of the exponent values (e_1,...,e_l) to at most one signature value (i, y, a).

10. A computer program element comprising program code means for performing a method of any one of the claims 1 to 9 when said program is run on a computer.

11. A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method according to anyone of the preceding claims 1 to 9.

12. A network device (p_i) comprising:

- a computer program product according to claim 11;

- a processor for executing the method;

- the processor having access to exchanged messages in the network.

* * *